United States Marine Corps
School of Advanced Warfighting
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

FUTURE WAR PAPER

AUTOMATED ACCESS AND ANALYSIS IN COUNTER NETWORK OPERATIONS

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF MASTER
OF OPERATIONS STUDIES

AUTHOR: LtCol Robert S. Ferguson USMC

AY 2006-2007

Mentor: Dr. Meyer

Approved: ___________________________

Date: ________________________________

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **2007**	2. REPORT TYPE	3. DATES COVERED **00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE **Automated Access and Analysis in Counter Network Operations**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **United States Marine Corps,School of Advanced Warfighting, Marine Corps University,2076 South Street, Marine Corps Combat Development Command,Quantico,VA,22134-5068**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**25**	

TABLE OF CONTENTS

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

EXECUTIVE SUMMARY

Title: Automated Access and Analysis in Counter Network Operations

Author: Lieutenant Colonel Robert S. Ferguson, United States Marine Corps.

Thesis: The US Intelligence Community (IC) must leverage the nation's unique information technology superiority and access to data in countering dark networked adversaries.

Discussion: The United States increasingly will likely oppose dark networked adversaries rather than only traditional nation states in future conflicts. These dark networked adversaries use a network form of organization and conduct activities that are both illegal and often secret. The IC, because of its Cold War hierarchical structure, is generally not as well equipped to counter this adversary as it is against a traditional nation state foe. Its hierarchical form limits effective information exchange. In order to counter dark networks more effectively, the IC must enable wider access to the large number of data sources both inside and outside US government control. This requires an examination of how it ensures information security and tags data for retrieval. Once the IC achieves wider data access, it must develop automated retrieval and analysis tools that can rapidly sort and link the large amount of data that would be available to intelligence analysts. These tools will facilitate improved understanding of dark networks adversaries and enable better decisions in future conflicts against them.

Conclusion: By leveraging wider access to global data and processing that data using automated retrieval and analysis tools, the IC will better understand the terrain of network adversaries, facilitating more informed counter network decisions.

Introduction

The US Intelligence Community (IC) must leverage the nation's unique information technology superiority and access to data in countering dark networked adversaries. In future conflicts, the US increasingly will oppose dark networked adversaries rather than only traditional nation states. In these conflicts, short of traditional warfare, the US's adversaries use network forms of organization and related strategies attuned to globalization and the information age.[1] Regrettably, the current organization of the IC inhibits effective operations against networked adversaries. This paper will first describe the organizational nature of the IC and the US's networked adversaries and why the IC has difficulty competing with those adversaries. It will then describe how wider access to intelligence and non-intelligence databases along with the use of automated retrieval and analysis tools can aid in countering those networks. These tools will facilitate improved understanding of dark networks and enable better decisions against them.

The IC and Adversary Organizational Forms

Organizational forms generally can be classified into two broad categories, hierarchies and networks. In hierarchies, every element in the organization is subordinate to another. This form is dominant among many large corporations and government bureaucracies, including US intelligence organizations. Because decision-making is often concentrated in a single entity, hierarchies' actions are more unitary and efficient because everyone works toward the same goals.[2] However, lines of communication run vertically, restricting or slowing information flow within the organization. In informational intensive activities, hierarchies with their restricted flow of information may not be the most competitive form of organization and may be outperformed by networks.[3] As a result, while hierarchical decisions are more unified and efficient they are comparatively less well informed in the information age.

The alternative organizational form, a network, is more effective in exchanging information than hierarchies. Networked organizations, consists of a web of dispersed interconnected nodes of individuals, groups, and organizations. Networks are flat, may not have a central leader, and have little or no central hierarchy.   The effectiveness of such an organization depends on a prevailing doctrine of ideology or common interests and objectives.[4] Unlike hierarchies, networks tend to thrive in an information rich environment; the more connections and greater the information flow, the stronger they generally become. Networks have an advantage in sharing observations and assessments, but since operations require consensus, decision-making is inefficient.[5] Networks, therefore, better understand the environment, but have difficulty taking unified rapid action.

A dark network, a term coined by Jorg Raab and H. Brinton Milward, describes a network that, unlike other social, political, or business networks, attempts to operate secretly outside of the law.[6] They engage in actions considered illegal by most governments such as acts of terrorism and drug smuggling.[7] These networks also operate secretly to hide their activities and ensure their survival. For example, Al Qaeda and the greater global Islamic insurgency is a dark network. Osama bin Laden has a small cadre within his immediate hierarchy, but the greater organization is a network controlled by a strong common ideology.   While Al-Qaeda does centrally coordinate some operations, its wider network operates based on a common ideology in the name of Al-Qaeda, often without central control or even with knowledge of the entire network.[8] Its principle activities are illegal and the network primarily operates secretly.

The IC is composed of hierarchical organizations whose traditional concept of operations relies on a centralized, top-down control and dissemination of information. The most sensitive information is normally restricted to only a few users. The community is made up of stovepiped organizations, which collect, store, analyze, and protect their own niche information.[9] This organizational approach, largely developed during the Cold War, compartmentalizes intelligence in order to protect information, sources, and collection methods.[10] It assumes the threat is well defined and not expected to radically change capabilities or methods of operations. Hierarchies operate well under these circumstances, since intelligence is primarily accessing current operations against other hierarchies, not developing new models.[11] This approach assumes it is possible to know who needs to use specific information and that broad intelligence sharing is risky. Information flows vertically from source, collector, database, and analyst to the consumer, normally in the form of a finished information product. A relic of the Cold War is, therefore, an intelligence system with a hierarchical proprietary information mentality.

A hybrid organizational model that informs using networks while maintaining hierarchical decision-making would be valuable in combating dark networks. In information rich environments, hierarchies such as US intelligence organizations are victims of abundant information and have a difficult time competing with dark networks that thrive on information abundance.[12] The organization that competes best against networked forms in the information realm are other networked organizations. Networked intelligence and information organizations are bettered suited to shape hierarchical decisions against poorly defined threats from multiple networked actors. Functions relating to decisions and actions, such as whether to conduct a strike operation, should remain hierarchical.[13] However, those functions requiring information exchange, like intelligence sharing and analysis, should operate in a more networked manner.[14]

Unfortunately, the IC does not store and process information effectively enough to operate in a competitive networked environment. It collects and stores vast amounts of information, both classified and unclassified. Adding other non-intelligence government and civil databases, the amount of information resident in a dispersed set of databases is immense. According to the 9/11 Commission, the IC has a very weak system to process and analyze all this data.[15] The Director of National Intelligence also believes IC analysts suffer from a lack of collaborative infrastructure and tools to minimize information overload.[16] The IC's poor ability to mutually access, process, and analyze data, allows dark networked adversaries to operate more freely.

Despite a tradition of information exclusivity, the IC - because of the US's current superiority in information technology - is uniquely positioned to overcome its information sharing and analysis issues. To do this, the IC first must leverage technology that facilitates greater access to intelligence, government, and civil data sources by the wider intelligence community. It also must concurrently design better methods to exploit the large amount of data that would be available through broader access by developing automated analytical tools able to process that data. Wider access and automated analysis together will greatly increase the intelligence community's ability to understand and counter dark networks.

Wider Networked Access

Wider access to intelligence and non-intelligence databases is essential to fighting dark networks. Much of the information needed to understand and fight dark networks resides in various non-associated intelligence databases. This is primarily due to dark networks' covert nature. Data collected by one organization may be valuable to another and dismissed. In other words, one intelligence organization may not know the significance or utility of the information it possesses. Analyzing the September 11th attacks reveals there was significant available data on both the hijackers and the operation before the attack.[17] The data was present, just dispersed in various intelligence and law enforcement databases. The network was secret and compartmented by design, which made putting the disparate data sets together only more difficult.[18] In addition, our adversaries conduct activities that produce information (such as phone and travel records) about themselves and their network during the normal conduct of both legitimate and illegitimate activities. That information is collected and stored in various non-intelligence databases. Such information is valuable in breaking networks, but is not readily available to the IC.

Wider automated access to databases is within current US technological capabilities. However, multiple issues impede wider data access. Two primary concerns are data format and information security. In order to facilitate widespread access, data must be in a format that is easily accessible. Specifically, data needs to be in an application independent format, so that multiple software applications can use them. Starting in October 2005, the IC mandated that the data format standard would be Extensible Markup Language (XML) for metadata (data about data) shared within national IC spaces.[19] The data standard ensures that data stored in the IC sphere is usable and searchable by multiple applications. Standardizing data facilitates automation. An intelligence report might have multiple pieces of data (names, addresses, and pictures); metadata tags each piece of data making retrieval easier. This standard is not enforced outside of the IC, and even within the IC not all data is tagged. As a result, a good deal of data, particularly legacy data, is still stored in non-standardized formats such as Microsoft products. For example, a tactical unit is not currently apt to meta tag a picture embedded in a PowerPoint slide stored on a local server. As a result, not only is it unlikely that external intelligence organizations know that the picture exits, but a wider intelligence network would have difficulty automatically ingesting that picture into analysis products. The picture is essentially only of value to the owners of that database or persons who know it exists. All data on government systems must be metadata tagged to ensure automated access to a wider community.

Another hurdle to wider information access is information security. Multiple US intelligence, defense, and other government agencies' databases, as well as databases owned by foreign governments and civil agencies, all have information of value for conducting analysis of dark networked organizations. However, many of these databases are not widely shared, partly due to concerns over information security. Among those that allow shared access, many restrict access to only a portion of the data or are only searchable through a stovepiped portal requiring specialized permissions. To allow for wider and more efficient use of information, intelligence databases have to be accessible by all users through a common portal allowing wider audience access, as opposed to the current model of access by exception.

Due to the secret nature of dark networks, the data needed to understand them does not exist solely in intelligence databases, but in the wider information pool composed of US government, foreign government, and civil databases. The IC, therefore, should have access to this data. This access must be consistent with Executive Order 12333 and DOD Directive 5240.1R stipulations that relate to collection on US entities by US intelligence personnel.[20] To accomplish this, either filters for US civil information or data anonymous files must be implemented before access to those databases are open to the intelligence community.[21]

The Joint Intelligence Operations Capability-Iraq (JIOC-I) developed by the US Army Intelligence and Security Command (INSCOM) has made large strides in database access and integration.[22] JIOC-I scrapes data from a designated network of servers into a large database, called the JIOC Brain. Several times a day it looks at those databases and websites and scrapes new data to update its database. JIOC-I users have access to that database. A search using JIOC-I would provide information from all those designated databases related to Iraq to include data from national intelligence agencies, theater agencies, and tactical websites located in Iraq.

Unfortunately, not all databases and servers are networked. JIOC-I may not be linked to civilian databases, independent tactical storage devices, other theater and government databases, and some intelligence databases that have restricted access.[23] In other words, some of the best tactical, national, and open source data may not be available to JIOC users.

JIOC does not automatically correlate data. It does come with analyst software, such as Pathfinder, Analyst's Notebook, Starlight, and ArcGIS, to allow easier manual analysis of the data.[24] A search using JIOC provides a list of files relevant to the search based on metadata related to the search subject. Generally, the analyst sees data files. While this is faster than previous methods of data searches and provides access to a larger pool of data, network analysis is still time intensive and requires manual manipulation and correlation of data. INSCOM fielded JIOC in Iraq in the summer of 2005 but is currently only resident on a US only domain. [25]

The next step in the evolution of a system following JIOC would be one with multiple security level access to all relevant data, not just a limited number of databases. Database access should include not just some theater or intelligence databases, but wider access to all relevant government, civilian, and foreign government sources of data. Any system with access to such data sources must have multilevel security to protect classified data, collection methods, and unclassified but sensitive data about individuals. The system should allow users access to all data at and below the level of their clearance access. Currently, clearance level alone is not sufficient to access sensitive information; the individual must have a need for the information. In a broader access system, there would no longer be a "need to know" stipulation for information sharing. For example, a user with Secret level access would have access to all Secret data and below on a single system. Here the presumption is the analyst needs the data rather than having a stipulated need to know to access specific information.

The strength of wider data access is that the data is now free to be used by a wide network of intelligence organizations. Data is no longer proprietary, but is treated like a commodity that can be used more frequently and efficiently; all analysts have access to the large pool of shared data, better ensuring it will be used. No longer are only a few hierarchies working a problem. Since the data is networked, it would follow that analysis of that data would also be networked, providing a richer source of understanding on the adversary network.

In order to be truly effective, this network should include intelligence, security, and law enforcement agencies of allies. Dark networks operate globally, often in places where some of the best information on their activities is collected by foreign governments or civil organizations. The benefit to the IC is access to a large pool of information collected by our allies. This effort would require a paradigm shift in the IC, but the risk that some data may be compromised is outweighed by the benefit more data. Since the US already has successful, secure, and long held intelligence sharing agreements with several allies, this risk is relatively small. Furthermore, multilevel security access will ensure "US Only" information stays in "US Only" domains.

Automated Analysis

With access to multiple databases, an automated method of retrieving and analyzing the large amount of information available on the network is needed. A key challenge with having large amounts of data on dark networks is that individual data points alone are meaningless. Data on networked organizations is relational. This means relevant information consists of relationships internal to and outside the network among people, places, things, and events.[26] Only together does the data describe, in any consequential, way a dark network's relationships.

The large amount of data available makes dark network analysis a difficult problem. Network analysis has traditionally been conducted manually. The advent of computerized tools such as Analyst Notebook and Starlight, which produce a graphic network representation based on relational data from a data source such as a spreadsheet, has made network analysis less tedious. However, network analysis still requires manual filtering of large quantities of data. Wider data access will make manual network analysis even more time consuming because of the increase in the amount data available to the analyst.   The IC should develop automated data mining and analysis tools connected to a distributed network to conduct that analysis.

Automated analysis is different from what is currently available on JIOC-I or traditional Internet query functions. JIOC-I's tools are an improvement, but they do not provide automated analysis of the data. These functions might find data sources or files based on a query, and may prioritize them based on importance, but they do not provide analysis or links within the various data available. Automated data analysis tools might help discern knowledge through links, associations, and patterns in raw data. This powerful capability will free analysts from the chore of searching through large and diverse sets of files looking for associations and allow them to spend more time conducting analysis.   There are several ways to use automated data searches to include subject-based analysis and pattern-based analysis.[27]

Subject-based analysis is a technique common in the intelligence community. A query could search a name, phone number, and location resulting in a link or association matrix that provides better understanding of the adversary network. As previously mentioned, intelligence organizations use computerized link analysis programs. (Appendix A)   However, these programs are not automated. The data is manually inputted and the links are built with human interaction. For example, a name subject search may currently identify a Signals Intelligence (SIGINT) report related to that name. The report may indicate two individuals contacted each other. That link is not automatically built, an analyst must read the report, identify an association, then build the link in a program. Analysts must then continue to search and manually identify additional links to those individuals in multiple files to build a picture of the network. Therefore, subject-based analysis, while indispensable to understanding a network, is a time intensive process that easily allows analysts to overlook links in networks because of the large amount of manually searched data.

There are currently programs that automatically conduct subject-based analysis by building links in data used by business and government. For example, some Las Vegas casinos use a program called Non-Obvious Relationship Awareness (NORA) developed by Systems Research & Development that correlates information, such as names, addresses, and surveillance camera images, within a database and detects links between casino personnel and known cheaters. NORA might indicate that a dealer’s maiden name or previous address matches that of a known cheater and link the two.[28] Rather than a time intensive manual search and analysis, the program automatically makes associations that may be several layers removed from the subject of the analysis. These programs require access to large standardized data sets to be effective.

Automated subject-based analysis would be an invaluable tool when combined with complete access to multiple databases. For example, a battalion intelligence section could quickly process data submitted via a personal digital assistant (PDA) on an individual stopped at a checkpoint. That section can take data sent by the checkpoint, such as his name or a picture, to determine any associated link or previous activity against a worldwide network of databases, not just localized information. An automated subject-based search may determine that he is using a false name, confirmed by biometric data stored in a theater database, or that he is associated with a known individual in an adversary network based on a combination of SIGINT data from NSA and imagery data from NGA.[29]   Currently, subject-based computer searches are easily defeated.

These searches do not have access to a full network of databases and manually searching and building links is a time prohibitive endeavor and only selectively conducted.

An additional function of automated subject-based analysis would be the ability to infer links between subjects. There may not be a direct piece of data linking the subjects of the analysis, but an inference might be based on the type of associations the two subjects have. For example, an automated subject-based analysis may identify a likely link between subjects based on a combination of common factors such as business associations or attendance at an event.

A subject-based query works well if there is a subject to search such as a person or location. However, secrecy is a characteristic of dark covert networks. These networks attempt to conceal their activity or presence. If the subject of a query is sufficiently concealed and its presence is unknown, a subject-based search and subsequent link analysis may not detect it. A key task, therefore, of counter network analysis is to infer the existence of a network and its activities based on data that relates people, places, things, and events. This is where an automated pattern-based analysis tool would be useful.[30]

Predictive or pattern of behavior analysis can help identify high-level behavior such as network organization and activities like the planning of an operation by using low-level data. In a subject-based analysis, both the data and inferences about individuals are known. In pattern-based analysis, the goal is to use data and activity inferences to make additional inferences about things that exist only at a higher level.[31] (Appendix B) Pattern-based analysis does not arise from interest in a person or place, but seeks information about persons, places, and things based on pattern of activity. For example, automated pattern-based analysis is commonly used to detect credit card fraud. The credit card company may determine that thieves commonly use stolen cards first to purchase a small amount of gas in order to validate that a card is good before making a large purchase. Automated pattern analysis might recognize that pattern and prompt further investigation on a card to determine if it is being used fraudulently.[32]

The strength of automated pattern-based analysis is not necessarily its power to describe relationships, but in making links in behavior that may indicate the possibility of future activity. While this type of automated analysis is common in business, its use is more difficult in countering dark networks. Private sector models attempt to find patterns among data from unrelated instances in a homogenous database and attempt to draw inferences from them. For example, a retailer might use unrelated data on customer purchases from its database to predict the type of purchase customers will make in the future and build inventory appropriately.

The nature of dark networks makes inferences more difficult. The data collected on dark networks tend to be key facts about associations between people, organizations, locations, and activities culled from a variety of different data sources, vice from one unitary database. Since wider dark networks are often composed of loose associations, a model for pattern-based analysis might need to find links among low-level activity, events, and people that exist in geographically dispersed locations to infer the dark network's activity.[33] For example, covert dark networks often act differently than normal social networks in that they form few new links outside of their network and keep existing ties to a minimum in order to maximize secrecy. Here, strong ties among elements of a dark network may only be internal.[34] An analyst might develop an automated pattern-based analysis to look for networks with sparse external connections. The model would filter and isolate that activity from networks forming many new outside connections. While sparse connections do not mean a dark network exits, it may stimulate further analysis or collection to determine the nature of the network.

Automated subject or pattern-based analysis will not replace human analysis and decision-making. These are simply tools to inform analysis and enlighten decision-making. Subject and pattern-based analysis are complex yet mundane tasks that computers do well. These tools certainly will not predict behavior nor will they provide an automatic indication of a specific activity. They can allow for a more thorough search of the vast amount of data available, aid in analysis, help determine if more detailed analysis is needed, and provide information to task additional intelligence collection. Free of the routine task of data searching, an analyst can spend time conducting higher-level analysis based on expertise and experience.

Counter Network Implications

By leveraging the vast amount of information available and applying automated tools to that data, the US will be in a better position to conduct operations against networked adversaries. While no amount of information will provide certainty to understanding a large network, using the data available in dispersed global data sources and conducting dispersed analysis will better enable actions that can effectively counter the network at large. Access to a large amount of shared data and analysis provides a common frame of understanding at all levels. Furthermore, by understanding how dark networks are organized and operate, the US can make better decisions on how and where to disrupt them.[35]

Common access to the vast amount of data on dark network activities will provide a common understanding of the network's landscape. This is akin to everyone having the same map. Currently tactical organizations have access to different data sets than national organizations. A regiment in Afghanistan might have very detailed data on the persons and events in that regiment's area of operations. Various national intelligence organizations have vast amounts of information; some of it might be pertinent to that regiment's area of operation.

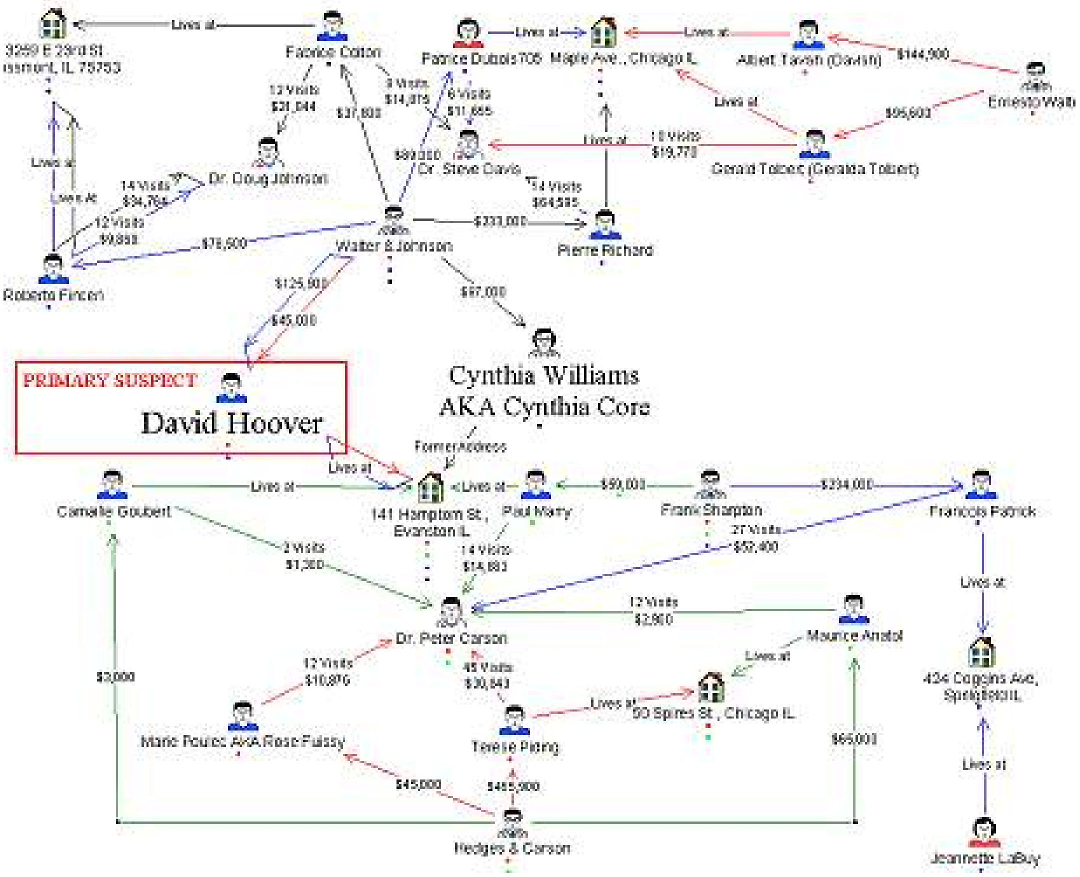
Both entities may have information relevant to the other; however, neither might know what the other has. If all units open their data sources to the wider network, all levels will have a richer base of data on which to conduct analysis. With a broader base of data, the local unit and national organizations will likely make more informed and synchronized decisions. For example, information from local patrols may indicate a local network node is using a café as a place to coordinate. National intelligence information may indicate a member of the local network who frequents that café is linked to a higher network. If the local commander does not understand that link, he may make a decision that jeopardizes exploitation of the larger network. National intelligence organizations might not have the detailed information the local unit has and may not have the clarity needed to exploit the data they are collecting. Automated database access precludes these stovepipes by providing a common map based on a shared data set. Each unit may use the map differently, but a common network map facilitates coordinated actions.

Shared data and analysis also facilitates the expeditionary nature of US military operations. Since all data would be easily and automatically available, analysis can occur at dispersed nodes. The benefit of shared data is a shared and living analysis. Analysts can automatically access shared analysis from a variety of sources to include past operations and build a communal and living analysis of a given location or activity regardless of the transitory nature of operation. For example, a Marine Expeditionary Force (MEF) in the conduct of an operation might access a global network of data and past analysis, combine that with locally collected data, and produce automated subject or pattern-based analysis. Based on experience in the operation, it might produce a synthesized product linked to the global set of data. Future units going to that area would access that analysis and modify it with acquire new information.

Understanding the network will ultimately permit the US and its allies to better design operations against them. By integrating large data sets and automated analysis to determine a network's topography, decisions on what node to disrupt become clearer. For example, if the network resembles a chain organization, disrupting any node will affect the network. (Appendix C) Better information will also lead to counter network operations that attack the strength of the network, its information flow. The network might be driven to an information poor environment, while the US moves to an information rich environment. The network will be information poor because the US's better informed actions are designed to disrupt the network. The network will realize this and attempt to limit its exposure by limiting interaction between nodes of the network. Since the strength of a network is its interactions, the networks capabilities diminish as its interactions are reduced.

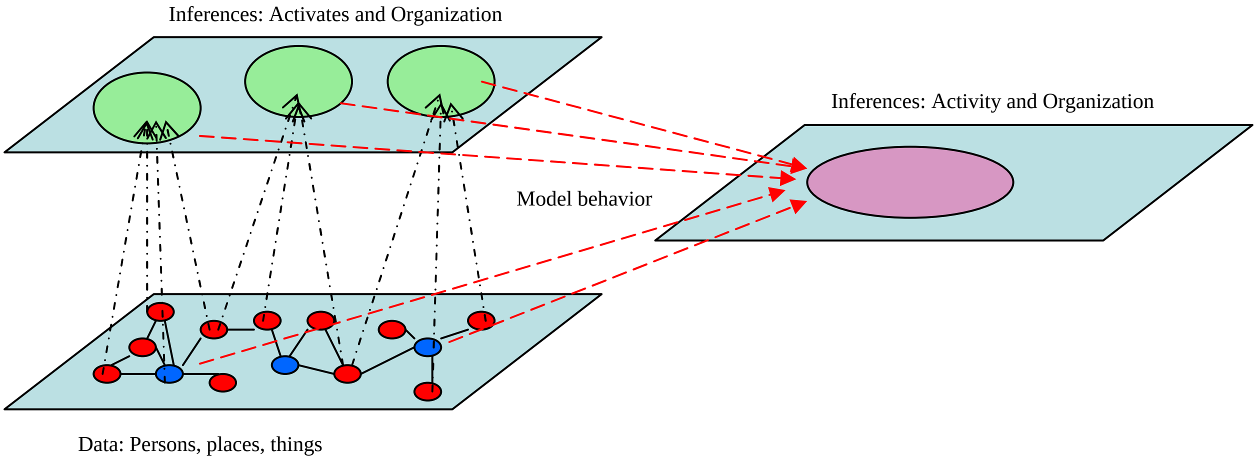
The US will likely continue to fight wars against covert and dark networked organizations. The IC's current design inhibits effective operations against networked organizations. Its hierarchical form limits effective information exchange. In order to combat networked organizations the IC must develop intelligence mechanisms that have better utility against them. Specifically, these mechanisms must use network forms of information sharing, allowing wider access to the vast amount of information available in US government, civil, and allied databases. To sort the large amounts of data available, automated analytical tools designed to combat networked adversaries should be emplaced. These will allow humans the ability to conduct analysis while allowing computers to conduct the mundane task of searching and correlating data. These tools ultimately will allow the US to better understand the terrain of network adversaries and facilitate better decisions in countering them.

Appendix A: Subject-based Analysis



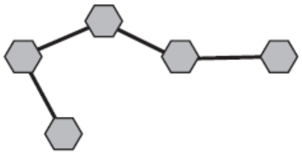
Subject-based Linked Analysis. The above is an example of a subject-based analysis, associating persons, things and locations using link analysis. Link analysis is a tool well suited for determining links between individuals to determine network organization.[36]

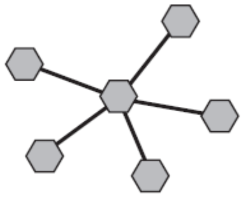
Appendix B: Pattern-based Analysis

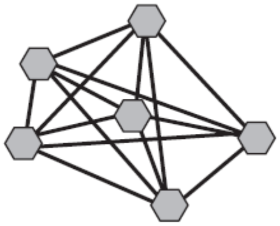

Inferences: Activates and Organization
Inferences: Activity and Organization
Model behavior
Data: Persons, places, things

Pattern-based Analysis. The above is an example a model for pattern-based analysis. Pattern-based analysis uses information from subject-based analysis combined with inferences to identify higher-level activity or organization.[37]

Appendix C: Network types


Chain network


Star or hub network


All-channel network

Network	**Description**	**Associated activity**	**Disruption**
Chain	People, goods, or information move along a line of separated contacts, and where end-to-end communication must travel through the intermediate nodes.	Drug or human smuggling	Disrupt any node or link
Star	Nodes are tied to a central node or actor, and must go through that node to communicate and coordinate.	Criminal franchise or a cartels, some insurgent/terrorist cells	Disrupt central node
All-channel	Every node is connected to the other nodes.	Militant peace groups insurgent/terrorist cells	Multiple nodes must be disrupted

[38]

[1] John Arquilla and David Ronfeldt, Networks and Netwars (Santa Monica CA: RAND, 2001), 6.

[2] John W. Bodnar, Warning Analysis for the Information Age: Rethinking the Intelligence Process (Washington D.C.: Center for Strategic Intelligence Research, December 2003), 60.

[3] John Arquilla and David Ronfeldt, In Athens's Camp (Santa Monica CA: RAND, 2001), 297.

[4] Arquilla and Ronfeldt, In Athens's Camp, 280.

[5] Bodnar, 60.

[6] Jorg Raab and H. Brinton Milward, "Dark Networks as Problems," Journal of Public Administration Research and Theory. (Oct 2003), 415. The term "Dark networks" coined in his article refers to organizations such as terrorist organizations, like Al Qaeda, drug networks, or transnational gangs.

[7] Not all governments will consider all actions illegal. For example, the Taliban in Afghanistan supported Al Qaeda whom conducted activities what most nations would consider terrorist acts.

[8] LtCol David Kilcullen, "Counter Global Insurgency, A Strategy for the Global War on Terrorism," (30 November 2004) 1. LtCol Kilcullen describes Al Qaeda as a networked transnational Islamic Insurgency. This means that it operates on a set of guiding principles and practices that allowing it to strive toward a common purpose such as remaking the world order, vice operating in centralized command or control manner.

[9] For example, the National Security Agency (NSA) specializes in Signals Intelligence (SIGINT) while the National Geospatial Intelligence Agency (NGA) focuses on geospatial intelligence. The intelligence Community can be divided into five categories: National Intelligence organizations such as the CIA, Department of Defense intelligence organizations such as the DIA, military service intelligence organizations such as MCIA, the intelligence components of the unified commands such as JICPAC, and civilian intelligence organizations like the FBI. Jeffery T. Richelson, The U.S. Intelligence Community, (Boulder CO: Westwiew Press, 1999), 12-13.

[10] David Steele, On Intelligence, (Oakton VA: OSS International Press, April 2002), 202.

[11] Bodnar 65.

[12] Arquilla and Ronfeldt, In Athens's Camp, 304.

[13] For example, time urgent functions, such as fire support, that require reactive behavior or functions whose effect if not properly controlled may have significant reverberating effects should continue to be executed by groups that are relatively hierarchical in nature.

[14] Arquilla and Ronfeldt, In Athens's Camp, 301.

[15] The 9/11 Commission Report, (New York, NY: W.W. Norton and Company Inc., 2004), 417.

[16] Director of National Intelligence. John D. Negroponte, Woodrow Wilson International Center for Scholars. Washington, DC. September 25, 2006.

[17]Valdis E. Krebs "Mapping Networks of Terrorists Cells", Connections. (24(3) 2002). Krebs has an excellent network analysis of the hijackers based on knowledge available at the time of the attack.

[18] Osama bin Laden stated, "Those who were trained to fly didn't know the others. One group of people did not know the other group." Transcript of Usama bin Laden Video Tape" December 13, 2001. http://www.defenselink.mil/news/Dec2001/d20011213ubl.pdf

[19] Timothy West, Intelligence Community Metadata Working Group, Data Interoperability Framework,, (17 December 2003). <http://web-services.gov/031217_OMB_ICMWG_DIF.ppt>, slide 6.

[20] These orders restrict US intelligence organizations from collecting on US persons and entities. While, not specially discussed in this article, EO 12333 and DODD 5240.1 ensures that intelligence personnel do not collect, retain, or disseminate information about US persons unless done in accordance with specific guidelines, proper authorization, and within only specific categories.

[21] Data anonymous files would be files on US persons and activities that do not betray the person's right to privacy against intelligence operations while still allowing the IC to use that data in network analysis.

[22] Its sister system, JIOC-A, is designed for operations in Afghanistan.

[23] Author visit to the Intelligence Operations Center, US Army Intelligence and Security Command (INSCOM) on 29 November 2006.

[24] United States Army Intelligence and Security Command, JOIC-I Technical Training Student Guide, (Newington VA, Lockheed Martin Information Technology: 2006). Analyst Notebook is a link analysis program, Pathfinder is a search program, ArcGis is a Geospatial program, and Starlight is a 3D analysis and visualization tool.

[25] Author visit to Intelligence Operations Center, INSCOM.

[26] David Jenson, Data Mining in Networks, (Washington, DC: December 11, 2002) <http://kdl.cs.umass.edu/people/jensen/papers/nrcdbsse02.html> slide 20.

[27] Mary DeRosa, Data Mining and Data Analysis for Counterterrorism, (Washington D.C.: Center for Strategic Studies, March 2004), 3.

[28] Kim Zetter, "Tracking Terrorists the Las Vegas Way," PCWorld.com. (7 Aug 2002). <http://pcworld.about.com/news/Aug072002id103692.htm>.

[29] Biometric Automated Toolset, BATS, is currently employed by the DOD to collect and store biometric data such as digital pictures and fingerprints on persons of interest and storing them on centralized servers in theater.

[30] Jenson, slide 21.

[31] Ibid.

[32] DeRosa, 4.

[33] DeRosa, 12.

[34] Krebs, 49.

[35] Kilcullen postulates there are only limited ways to effectively attack a global networked insurgency. These include attacking the networks nodes, interdicting its links, suppressing boundary interactions, choking off inputs, and denying outputs to the network. Unless the networks are well understood decisions to operate on these nodes, links and boundaries will be ill informed.

[36] i2 Inc. Analyst's Notebook example of Analyst's Notebook link analysis from <http://www.i2inc.com/Products/Analysts_Notebook/default.asp#>.

[37] Jenson, slide 22.

[38] John Arquilla and David Ronfeldt, Networks and Netwars 8.

Works Cited

Arguilla, John and David Ronfeldt. Networks and Netwars. Santa Monica CA: RAND, 2001.

Arguilla, John and David Ronfeldt. In Athens's Camp. Santa Monica CA: RAND, 1997.

Bodnar, John W. Warning Analysis for the Information Age: Rethinking the Intelligence Process. Washington D.C.: Center for Strategic Intelligence Research, December 2003.

DeRosa, Mary. Data Mining and Data Analysis for Counterterrorism. Washington D.C.: Center for Strategic Studies, March 2004.

Department of Defense. DOD Intelligence Activities. DODD 5240.1R. Washington DC: April 25, 1988.

i2 Inc. Analyst's Notebook. <http://www.i2inc.com/Products/Analysts_Notebook/default.asp#>. [3 December 2006]

Jenson, David. Data Mining in Networks. Washington, DC: December 11, 2002, <http://kdl.cs.umass.edu/people/jensen/papers/nrcdbsse02.html>. [November, 15 2006].

Kilcullen, David LtCol. "Counter Global Insurgency, A Strategy for the Global War on Terrorism" 30 November 2004.

Krebs, Valdis E. "Mapping Networks of Terrorists Cells", Connections. (24(3) 2002) 43-52.

Negroponte, John D. Director of National Intelligence, Woodrow Wilson International Center for Scholars. Washington, DC. September 25, 2006.

Raab, Jorg and H. Brinton Milward. "Dark Networks as Problems." Journal of Public Administration Research and Theory. (Oct 2003) 413-439.

Richelson, Jeffrey T. The U.S. Intelligence Community. Boulder CO: Westview Press, 1999.

Steele, David. On Intelligence, Oakton VA: OSS International Press, April 2002.

The 9/11 Commission Report, New York, NY: W.W. Norton and Company Inc., 2004.

United States Army Intelligence and Security Command. JOIC-I Technical Training Student Guide. Newington VA: Lockheed Martin Information Technology, 2006.

U.S. President. Executive Order US Intelligence Activities, EO 12333. Washington D.C.: 4 December 1981.

United States Department of Defense. “Transcript of Usama bin Laden Video Tape” December 13, 2001. http://www.defenselink.mil/news/Dec2001/d20011213ubl.pdf

West, Timothy, Chair IC Metadata Working Group. Intelligence Community Metadata Working Group, Data Interoperability Framework.17 December 2003. <http://web-services.gov/031217_OMB_ICMWG_DIF.ppt> [20 November 2006].

Zetter, Kim. “Tracking Terrorists the Las Vegas Way.” PCWorld.com. 7 Aug 2002. <http://pcworld.about.com/news/Aug072002id103692.htm>. [15 November 2006].